IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. JAMES GORDON MEEK *Defendant*.	Case No. 1:23-cr-65

UNITED STATES' OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS CONTENTS OF DEFENDANT'S INTERNET ACCOUNTS

The defendant moves this court to suppress the contents of his internet accounts on the grounds that they were illegally seized pursuant to preservation requests issued to providers under 18 U.S.C. § 2703(f). Preservation requests do not violate the Fourth Amendment, and even if they did, suppression is not an appropriate remedy. The defendant's motion should be denied.

RELEVANT BACKGROUND

A. Facts

The investigation into the defendant's criminal conduct originated with a report by Dropbox indicating that Dropbox had detected child sexual abuse material (CSAM) in the defendant's Dropbox account. The Federal Bureau of Investigation opened an investigation. As the FBI identified accounts relevant to the investigation, the FBI sent preservation requests to various electronic communication service and/or remote computing service providers (collectively, the providers) requesting to preserve those accounts pending further investigative action.

The defendant now challenges preservation requests sent regarding 14 accounts, claiming the requests violated the Fourth Amendment and seeking the suppression of the "entire contents" of those accounts. ECF No. 53 at 1; *see also* ECF No. 53 at 1-2 (chart identifying accounts and associated preservation requests the defendant is challenging). Notably, the government only obtained the contents of three of the accounts identified. For the other 11 accounts for which the government sent a preservation request, the government subsequently either received only non-content information (such as subscriber records, IP address logs, and/or email routing information), or no information at all.

Specifically, on November 14, 2022, the government obtained search warrants authorizing the seizure and search of the contents of the following three accounts:

- Apple iCloud account associated with [redacted]
- Apple iCloud account associated with [redacted]
- Snapchat account associated with the username "[redacted]"

The preservation request for the "[redacted]" Snapchat account was sent on October 4, 2022. Snap[1] sent its acknowledgement of the request on October 7, 2022. The oldest content provided in response to the "[redacted]" search warrant was dated October 21, 2022.

B. Statutory background

The Stored Communications Act, 18 U.S.C. §§ 2701-2713, regulates access to and disclosure of stored communications and other information held by network service providers. The first three subsections of § 2703 specify procedures that a governmental entity may use to compel

[1] The application Snapchat is offered by a company called Snap, Inc.

a communication service provider to disclose various categories of information pertaining to a subscriber or customer. *See* 18 U.S.C. § 2703(a)-(c). Pursuant to Section 2703(a) and (b), the government must obtain a search warrant to obtain content information; however, the government may obtain information such as basic subscriber information and IP address information with a subpoena, *see* § 2703(c)(2), or other records, including email to/from data, with a court order, *see* § 2703(d).

Section 2703(f) allows a governmental entity to request that a service provider preserve records temporarily. It states that a service provider, "upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process." 18 U.S.C. § 2703(f)(1). The provider is required to retain preserved information for 90 days, and the governmental entity may request a 90-day extension. *See* 18 U.S.C. § 2703(f)(2).

After the period of required preservation ends, the provider is free to delete the preserved information. Preservation requests do not apply prospectively: the provider's duty to preserve is limited to information that the provider already had in its possession when it received the preservation request. Finally, § 2703(f) does not mandate a specific manner of preservation.

ARGUMENT

The defendant's motion fails at every step of the analysis. First, the defendant has no Fourth Amendment standing to seek suppression of any non-content records obtained by the government, including for the 11 accounts for which the government did not receive content. Second, even as to the three accounts for which the government ultimately obtained content, preservation requests do not violate the Fourth Amendment. That is because the preservation of the content is not a government action, a preservation is not a search or seizure, the providers had authority to create

copies of the account and the defendant consented to that action, and preservation is reasonable. Finally, even if the preservation did constitute a Fourth Amendment violation, suppression is not appropriate because the good-faith exception applies, and the defendant cannot establish the requisite but-for causation between the preservation and the government ultimately obtaining the data.

A. The defendant has no Fourth Amendment standing to seek suppression of non-content records.

As an initial matter, the defendant has no reasonable expectation of privacy in any non-content records, including subscriber information, IP addresses, or email to/from data, produced to the government. As a result, there is no basis for suppression of any non-content materials.[2] "[A] defendant 'has no expectation of privacy in IP addresses' or basic subscriber information because internet users 'should know that this information is provided to and used by Internet service providers for the specific purpose of directing and routing information.'" *Rosenow*, 50 F.4th at 738 (quoting *United States. v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008)); *see also United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) (no expectation of privacy in subscriber information because it is "voluntarily conveyed" to a third party); *United States v. Wellbeloved-Stone*, 777 Fed. App'x 605 (4th Cir. 2019) (holding "no reasonable expectation of privacy in [defendant's] IP address or subscriber information"); *United States v. Ulbricht*, 858 F.3d 71, 97 (2d Cir. 2017) (*abrogated on other grounds*); *United States v. Caira*, 833 F.3d 803, 806 (7th Cir. 2016). Similarly, individuals have no expectation of privacy in the to/from lines of emails that are

[2] Moreover, to the extent that the government did not obtain any information at all about an account, there is nothing to suppress.

provided in response to a § 2703(d) order: this information is analogous to the "information people put on the outside of an envelope" which is "voluntarily transmitted to third parties," therefore obliterating any privacy expectation. *Rosenow*, 50 F.4th at 738. Because the defendant has no privacy expectation in the non-content data, there can be no Fourth Amendment violation. Suppression is not available as to these records.

B. The preservation requests did not violate the Fourth Amendment.

The government ultimately obtained content for three different accounts—two Apple accounts and one Snapchat account. However, the preservation requests did not violate the Fourth Amendment because (1) they did not create an agency relationship and the Fourth Amendment does not reach private action, (2) a preservation request is not a Fourth Amendment search or seizure, (3) the defendant consented to the copying of the accounts, and (4) the preservation was reasonable.

1. The preservation requests did not create an agency relationship.

The defendant's argument that the preservation request violated the Fourth Amendment fails because preservation does not create an agency relationship. The Fourth Amendment does not reach conduct by a private individual not acting as an agent of the government. *See United States v. Jacobsen*, 466 U.S. 109, 113 (1984). When a party merely complies with a legal duty to preserve information in its possession, it does not become a government agent. For example, all taxpayers are required to keep tax records, *see* 26 U.S.C. § 6001, but such a requirement does not transform all taxpayers into government agents. Nor does 18 U.S.C. § 1519, which criminalizes knowingly destroying records with intent to obstruct a federal investigation, convert everyone in possession of such records into government agents.

The Supreme Court has come to the same conclusion in a similar context. In *California Bankers Association v. Shultz*, 416 U.S. 21 (1974), the Supreme Court considered constitutional challenges to the Bank Secrecy Act and associated regulations that required banks to keep, for a period of years, specified records useful in criminal investigations. *See* 12 U.S.C. § 1829b(g). Banks argued that the Act was unconstitutional because it made "the banks the agents of the Government." *California Bankers Ass'n*, 416 U.S. at 45. The Supreme Court dismissed this argument, explaining that "[s]uch recordkeeping requirements are scarcely a novelty." *Id.* This analysis did not change even though the purpose of the recordkeeping requirement extended beyond bank regulation to include aiding criminal investigations. *Id.* at 47.

In support of his argument, the defendant cites *Commonwealth v. Gumkowski*, 167 N.E. 3d 803 (Mass. 2021) and *United States v. Hardin*, 539 F.3d 404 (6th Cir. 2008), but those cases are clearly distinguishable and involved more significant and invasive conduct that did result in an agency relationship. In *Gumkowski*, a company disclosed cell-site information to the government without the required warrant, while in *Hardin*, an apartment manager entered the defendant's home upon the request of the police. In both cases, the private actor voluntarily engaged in substantial and intrusive conduct that directly furthered the investigation at the government's request. Here, the private actors fulfilled their limited statutory obligation to keep certain information on hand for a short period of time. The government only obtained that information after a search warrant was issued; the government did not request that any provider review the defendant's account or otherwise directly assist with the investigation. Thus, the cases do not support the argument that any providers were agents of the Government when they preserved the defendant's accounts. Nor do they support the defendant's suggestion that any request from the government, no matter how minor or routine, effectively converts private actors into state actors.

2. A preservation request is not a Fourth Amendment seizure.

The defendant's challenge to the preservation request fails also because a preservation request is not a seizure.[3] "A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). But when the government sends a preservation request to a service provider, it obtains no information at all, and the account owner retains full and unhindered access to his account. In addition, § 2703(f) includes no general recordkeeping requirements; a 2703(f) request requires only temporary preservation of information that the provider has already chosen to store. This temporary mandate does not constitute a meaningful interference with an account holder's possessory interests.

The defendant claims that prior to his accounts being preserved he had control over his accounts, including the ability to view, alter, and delete his files. Yet a preservation request does not impact a person's ability to use their account, to view, alter, or delete their files. It is merely a snapshot of the account as it existed at the time the preservation request is received. Nor does a preservation request result in the government gaining control of the data; the government cannot view, alter, or delete those files. Particularly when considering that the preservation requests were submitted after the defendant's crimes had occurred as part of the investigation, the defendant is essentially arguing that he should have the right to obstruct justice by deleting his data at any time.

The cases cited by the defendant do not support his argument. In *United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002), the court considered whether an email provider's execution of a

[3] The defendant concedes that a preservation request is not a search. *See* ECF No. 53 at 11.

search warrant violated the Fourth Amendment. The fact that this was a search and seizure was uncontested—the government had obtained a warrant and received the full contents of the defendant's account. The actual question presented was whether the Fourth Amendment required law enforcement to be physically present. *See id.* at 1066-67. That question is not at issue here. In *Vaugh v. Baldwin*, 950 F.2d 331 (6th Cir. 1991), the question presented was whether the government could keep documents after consent was withdrawn and copy documents not lawfully in its possession. Here, of course, the preserved materials are not in the government's possession, lawfully or otherwise, the government is not doing the copying, and the government does not end up with the content at the end of the copying. And in *United States v. Loera*, 333 F. Supp. 3d 172 (E.D.N.Y. 2018), the court expressly concluded that copying does not "interfere with a *possessory* interest because copying does not damage the data or interfere with its owner's ability to use it." *Id.* at 185. And it is precisely that possessory interest that is in question here. *See Jacobsen*, 466 U.S. at 113.

In fact, the only judicial decision to address the constitutionality of a § 2703(f) preservation request found no Fourth Amendment violation. In *United States v. Rosenow*, No. 17-cr-3430, 2018 WL 6064949, at *10 (S.D. Cal. Nov. 20, 2018) (affirmed on other grounds by the Ninth Circuit), the court found that preservation requests "did not interfere with the Defendant's use of his accounts and did not entitle the Government to obtain any information without further legal process." The court concluded that the requests "did not amount to an intrusion subject to Fourth Amendment requirements." *Id.* Moreover, the defendant fails to cite any case holding that a preservation mandate constitutes a seizure or a search.

Related Supreme Court case law reinforces the conclusion that preservation requests are not seizures. In *California Bankers Association*, 416 U.S. at 52, banks and others argued that their

Fourth Amendment rights were violated by the preservation requirements of the Bank Secrecy Act. Although bank depositors have no Fourth Amendment interests in records held by a bank, a bank itself certainly has Fourth Amendment interests in its own papers. Yet the Court held that "[w]e see nothing in the Act which violates the Fourth Amendment rights of any of these plaintiffs" because none of the record keeping rules "require that any information contained in the records be disclosed to the Government." *Id.* In fact, as with the preservation statute, "access to the records is to be controlled by existing legal process." *Id.* Third-party preservation alone is simply not a Fourth Amendment concern.

To be sure, *California Bankers Association* is potentially distinguishable because it involved "transactions to which the bank was itself a party." 416 U.S. at 52. But whether a preservation mandate amounts to a seizure should not be affected by whether the mandate is directed to an individual or to an entity that the individual has chosen to store her records.

In addition, copying information pursuant to a preservation request does not violate the Fourth Amendment under the reasoning of *Arizona v. Hicks*, 480 U.S. 321, 324-25 (1987). In *Hicks*, the Supreme Court held that an officer moving stereo components conducted a search, but that his recording of the components' serial numbers was not a seizure. The officer in *Hicks* conducted a search because he lacked authority to move the components and "exposed to view concealed portions of the apartment," conduct which does not occur pursuant to a preservation request. *Id*. at 325. More significantly, the Court explained that recording the numbers did not amount to a seizure because it "did not 'meaningfully interfere' with respondent's possessory interest in either the serial numbers or the equipment." *Id*. Similarly, to the extent that a provider copied the defendant's accounts pursuant to the preservation request, that provider did not meaningfully interfere with the defendant's possession of it, as he remained free to use the account

for whatever purposes he deemed fit. Thus, preservation of the defendant's accounts was not a seizure.

3. The providers had authority to create copies of the accounts, and the defendant consented to such action.

Even if preservation of the defendant's accounts were a seizure, it would not violate the Fourth Amendment both because the providers had authority to create copies of the defendant's information and because the defendant had consented. It is well settled that consent is an exception to the Fourth Amendment's warrant requirement. *See Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973).

As an initial matter, a search or seizure can be authorized by a third party who has "common authority over or other sufficient relationship to" the items in question. *United States v. Buckner*, 473 F.3d 551, 554 (4th Cir. 2007) (quoting *United States v. Matlock*, 415 U.S. 164, 171 (1974)). In the context of authorizing a search, that authority requires that the third party have "joint access or control for most purposes" such that it is "reasonable to recognize that any of the co-[users] has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common [effects] to be searched." *Matlock*, 415 U.S. at 171 n.7. Here, the providers had a sufficient relationship to the defendant's accounts to consent to the much less intrusive act of preserving their contents. That is because providers regularly copy, preserve, and store data in the course of their own business activities. In fact, for a cloud storage provider like Apple, creating copies and back-ups is the entire purpose of the service. It is thus "reasonable to recognize" that these providers may take these same actions at the government's request.

Moreover, the defendant expressly "assumed the risk," *Buckner*, 473 F.3d at 554, of providers preserving his data when he consented to it in the providers' Terms of Service. A service provider's terms of service can establish subscriber consent. *See, e.g.*, *United States v. Adkinson*, 916 F.3d 605, 610 (7th Cir. 2019) (rejecting Fourth Amendment challenge to disclosure of cell phone location information in part because defendant "agreed to T- Mobile's policy that T-Mobile could disclose information when reasonably necessary to protect its rights, interests, property, or safety").

Here, both Apple and Snap give users permission to use their services if users agree to follow specific terms. *See* Apple, *Welcome to iCloud*, available at https://www.apple.com/legal/internet-services/icloud/; Snap Inc. Terms of Service, available at https://snap.com/en-US/terms. These terms expressly provide that both Apple and Snap may preserve user data in response to government requests. Specifically, Apple's terms provide that "Apple may . . . access, use, preserve, and/or disclose your Account information and any Content to law enforcement authorities . . . if legally required to do so." Snap's terms of service incorporate its privacy policy, which provides, "There may be legal requirements to store your data . . . if we receive valid legal process asking us to preserve content," among other reasons. These terms expressly cover the providers' preservation at issue here.

Once again, the cases the defendant cites do not suggest otherwise. In both *United States v. Byrd*, 138 S.Ct. 1518 (2018), and *United States v. Washington*, 573 F.3d 279 (6th Cir. 2009), the courts concluded that a contract violation did not mean a defendant had no Fourth Amendment rights. But in neither of those cases had the defendants expressly consented to the action in question—as the defendant had here.

The defendant thus tries to call the entire concept of his consent into question, claiming that users do not read terms of service. ECF No. 53 at 14. But courts "uniformly hold that 'failure to read an enforceable contract, as with any binding contract, will not excuse compliance with its terms.'" *Hosseini v. Upstart Network, Inc.*, 19-cv-704, 2020 WL 573126, at *5 (E.D. Va. Feb. 5, 2020) (Ellis, J.) (quoting *Feldman v. Google, Inc.*, 513 F. Supp. 2d 229, 236 (E.D. Pa. 2007)); *see also One Beacon Ins. Co. v. Crowley Marine Servs., Inc.,* 648 F.3d 258, 270 (5th Cir. 2011) ("[T]he fact that a party chooses not to review a contract, or terms and conditions, when they had the opportunity does not negate the fact that they are bound by those Terms and Conditions."); *Schwartz v. Comcast Corp.,* 256 Fed.Appx. 515, 520 (3d Cir. 2007) (a customer on notice of contract terms available on the internet website is bound by those terms). Because these terms were readily available and clearly stated that users consent to preservation, the defendant's consent is valid and enforceable.

Because the defendant agreed that Apple and Snap could preserve his accounts as a condition of him using their services, that preservation does not violate the Fourth Amendment.

4. Preservation was reasonable.

Even if this Court were to find that preservation requests are seizures to which the defendant did not consent, they would not violate the Fourth Amendment because they are reasonable. The Supreme Court has recognized that "[i]n some circumstances, such as '[w]hen faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable.'" *Maryland v. King*, 569 U.S. 435, 447 (2013) (quoting *Illinois v. McArthur*, 531 U.S. 326, 330 (2001)); *see, e.g.*, *United States v. Jacobsen*, 466 U.S. 109, 125 (1984) (holding that destruction of powder used in field test was reasonable, despite being a

warrantless seizure). Furthermore, at a minimum, *California Bankers Association* establishes that a statute mandating the preservation of records need not include a search warrant requirement. Thus, if preservation requests are subject to Fourth Amendment scrutiny at all, courts should "balance the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable." *Maryland v. King*, 569 U.S. at 448.

The privacy impact of preservation requests on account holders is minimal. Preservation requests do not result in disclosure of information. They do not result in collection of information not already stored by the provider. They do not hinder an account holder's access to or use of his account. Their duration is brief, and afterwards the provider is free to delete the preserved information. In addition, the government must still obtain appropriate legal process, such as a search warrant, in order to actually obtain any information from or about the account.

On the other side of the balance, as Congress has recognized, the government has a compelling interest in preservation requests. Electronic evidence is critical in a wide range of criminal investigations, and it can be deleted irretrievably in an instant. The procedures of 18 U.S.C. § 2703 allow the government to ensure that critical data is not lost while it obtains appropriate process to compel disclosure of the information. Preservation requests also play a critical role in other important circumstances, such as investigations by foreign countries of crime: § 2703(f) allows the United States to request that service providers preserve data while foreign countries pursue the lengthy Mutual Legal Assistance Treaty process.

Balancing these interests, the preservation provisions of § 2703(f) are reasonable. Moreover, this conclusion is bolstered by the "strong presumption of constitutionality" of federal statutes challenged on Fourth Amendment grounds. *United States v. Watson*, 423 U.S. 411, 416 (1976). The preservation of the defendant's accounts did not violate the Fourth Amendment.

C. Even if preservation violates the Fourth Amendment, suppression is not an appropriate remedy.

Even if this court were to hold that preservation letters violated the Fourth Amendment, suppression is not an appropriate remedy because (1) the good-faith exception applies and (2) the defendant cannot establish but-for causation.

1. The good-faith exception applies.

Even if the preservation in this case violated the Fourth Amendment, suppression would not be an appropriate remedy. In *Illinois v. Krull*, 480 U.S. 340, 349-50 (1987), the Supreme Court held that the good-faith exception to the exclusionary rule applies where law enforcement reasonably relies on a statute later determined to be unconstitutional. *See also United States v. Korte*, 918 F.3d 750, 757-59 (9th Cir. 2019) (applying Krull to reject suppression of cell-site information obtained in good-faith reliance on 18 U.S.C. § 2703(d)); *United States v. Warshak*, 631 F.3d 266, 288-92 (6th Cir. 2010) (holding that government relied in good faith on 18 U.S.C. § 2703 in compelling disclosure of email content with a subpoena and court order). Moreover, this Court may conclude that officers relied in good faith on a statute without resolving the statute's constitutionality. See, e.g., *United States v. Vanness*, 342 F.3d 1093, 1098 (10th Cir. 2003).

Krull applies here because the United States followed § 2703(f) when it sent a preservation request to the providers, and because no court has ever found this provision unconstitutional. The United States did exactly what the statute authorizes, requested preservation, which the provider was required by statute to retain for 90 days. Because the United States reasonably relied on the procedures of § 2703, *Krull* precludes suppression of the evidence from the defendant's Apple and Snapchat accounts.

The defendant's attempts to distinguish *Krull* make no sense. As the defendant himself states, the "preservation request statue was enacted to ensure government access to user records that might otherwise be deleted before the government obtained legal process." ECF No. 53 at 4. But under the defendant's proposed reading of the statute, the government is only free to send a preservation request if it has already obtained a search warrant—at which point, of course, preservation is no longer useful. This court cannot adopt a reading of the statute that would turn § 2703(f) "into nothing more than surplusage." *Nero v. Mosby*, 890 F.3d 106, 124 (4th Cir. 2018). Moreover, § 2703(f) is materially indistinguishable from the statute at issue in *Krull*, in the sense that both statutes authorized government actions—here, preservation letters; in *Krull*, inspection of books and records—without making any statement about what legal process might be required. The Supreme Court nonetheless concluded that Congress, not law enforcement, had erred, and that the government had acted in good faith in relying on the statute.

2. The defendant does not and cannot demonstrate that preservation was the "but-for" cause of the government obtaining the evidence.

"A Fourth Amendment violation requires suppression of evidence only if the violation is the "but-for" cause of the government obtaining the evidence. *United States v. Rosenow*, 50 F.4th 715 (9th Cir. 2022) (citing *Hudson v. Michigan*, 547 U.S. 586, 592 (2006) (explaining "but-for causality" is a necessary condition for suppression of evidence)).[4] But the defendant does not allege and cannot establish the requisite causation. As an initial matter, the defendant does not allege that he deleted or attempted to delete materials that were then only recovered as a result of

[4] Even then, "but-for causality is only a necessary, not a sufficient, condition for suppression." *Hudson*, 547 U.S. at 592. In light of the good-faith exception, even but-for causality would not be sufficient here.

the preservation request. Nor does he allege that the government even received preserved copies of the accounts, instead of copies of the accounts made at the time of warrant execution. In fact, while Snap acknowledged the government's preservation request on October 7, 2022, the *oldest* data that was produced from the Snapchat account was dated October 21, 2022, and therefore would not have been copied in response to the government's request. The defendant cannot establish a necessary condition for suppression, and his motion should be denied.

CONCLUSION

For the reasons stated above, the defendant's motion to suppress should be denied.

Respectfully submitted,

Jessica D. Aber
United States Attorney

By: /s/

Zoe Bedell
Assistant United States Attorney
Whitney Kramer
Special Assistant United States Attorney (LT)
United States Attorney's Office
2100 Jamieson Ave.
Alexandria, Virginia 22314
Phone: 703-299-3700
Email: Zoe.Bedell@usdoj.gov